Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-20 (canceled without prejudice)

21. (new) A method for secure data transfer in a wireless networked communication system, the method comprising the acts of:

generating an encryption key within a first device of the communication system;

encoding the encryption key to form an encoded encryption key signal;

wirelessly transmitting the encoded encryption key signal to a second device of the communication system remote from the first device, wherein the first device and the second device are confined within a room;

decoding the encoded encryption key signal at the second device to extract the encryption key; and

using the encryption key to encrypt and decrypt data for subsequent wireless transmissions between the first and second devices;

wherein the encoded encryption key signal is not readily detectable outside of the room.

22. (new) The method of claim 21, wherein the encoded encryption key signal comprises an acoustic signal.

23. (new) The method of claim 22, wherein the acoustic signal comprises DTMF tones.

24. (new) The method of claim 21, wherein the encoded encryption key signal comprises an infrared signal.

25. (new) The method of claim 21, wherein the act of decoding further comprises the act of storing the decoded encryption key in memory.

26. (new) The method of claim 21, wherein the act of decoding further comprises the act of performing error detection to determine if an error has occurred in connection with the reception or decoding of the encryption key.

27. (new) The method of claim 26, further comprising the act of sending a request for a retransmission of the encoded signal if an error is detected.

28. (new) The method of claim 21, wherein the act of using the encryption key to encrypt and decrypt subsequent wireless transmissions further comprises the act of encoding the data into radio frequency signals.

29. (new) The method of claim 21, further comprising the act of determining whether a new encryption key is required.

30. (new) A system for secure data transmission within a wireless communication system, comprising:

a first device of the communication system, the first device having an encryption key generator for generating the encryption key and a signal transmitter for wirelessly transmitting an encoded signal representative of the encryption key; and

a second device of the communication system, the second device having a signal sensor for receiving the encoded signal from the first device and a decoder device for extracting the encryption key from the encoded signal, the encryption key being used to encrypt data being wirelessly transmitted between the first and second devices;

wherein the first device and the second device are confined within a room; and

wherein the encoded signal representative of the encryption key is not readily detectable outside of the room.

31. (new) The system of claim 30 wherein the first device further comprises an encoder device for encoding the encryption key into an encoded encryption key signal for transmission.

32. (new) The system of claim 31 wherein the encoder device comprises an acoustic codec.

33. (new) The system of claim 10, wherein the encoded encryption key signal comprises an acoustic signal.

34. (new) The system of claim 30, wherein the signal transmitter comprises an acoustic transmitter, and wherein the signal sensor comprises an acoustic sensor.

35. (new) The system of claim 30, wherein the decoder device comprises an acoustic codec.

36. (new) The system of claim 30 further comprising memory in the first and second devices for storage of the encryption key.

37. (new) The system of claim 30 further comprising an encryption/decryption module in the first and second devices for encrypting data for transmission and decrypting data received from the other device.

38. (new) The system of claim 30 further comprising a radio-frequency codec in the first and second devices for encoding the data into radio-frequency signals.

39. (new) The system of claim 38 further comprising a radio-frequency transceiver in the first and second devices for transmission and reception of the radio-frequency signals within the communication system.

40. (new) A system for secure data transmission within a wireless communication system, comprising:

means for generating an encryption key within a first device of the communication system;

means for encoding the encryption key to form an encoded encryption key signal;

means for wirelessly transmitting the encoded encryption key signal to a second device of the communication system remote from the first device, wherein the first device and the second device are confined within a room;

means for decoding the encoded encryption key signal at the second device to extract the encryption key; and

means for using the encryption key to encrypt and decrypt data for subsequent wireless transmissions between the first and second devices;

wherein the encoded encryption key signal is not readily detectable outside of the room.